

UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the
person by name and address)

4827 RIVERTON AVENUE
NORTH HOLLYWOOD, CALIFORNIA

Case No. 2:24-MJ-7119

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A

located in the Central District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §§ 1341, 1343, 1344, 1349, 1956, and 1957. See affidavit 1546.

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days: _____*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s Jenae Combest-Smith

Applicant's signature

Special Agent Jenae Combest-Smith , HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date:

Judge's signature

City and state: Los Angeles, CA

Hon. Margo A. Rocconi, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A-1

THE PREMISES TO BE SEARCHED IS:

4827 RIVERTON AVENUE, NORTH HOLLYWOOD, CA 91601 and its attached garage (the "SUBJECT PREMISES"). The SUBJECT PREMISES is a three-story townhome that is attached to another unit with a different street number, 4829. The townhome complex is located on the west side of RIVERTON AVENUE between Peach Grove Street and Camarillo Street. It is finished in stucco, with the first floor painted in gray and the second and third floors painted in tan/beige. The second story of the SUBJECT PREMISES contains a balcony. The townhome building includes garaged parking behind the building. There is a black gate on the right side of the building, which provides access to the garages and the back of the building. The door to the SUBJECT PREMISES is white in color and is marked by the numbers "4827" in black above the door. The premises to be searched includes all of 4827 RIVERTON and any vehicles located in its attached garage.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1341, 1343, 1344, 1349, 1956, and 1546 (conspiracy to commit mail, wire, and bank fraud, money laundering, and passport fraud), collectively referred to as the "SUBJECT OFFENSES," namely:

a. Documents and records referring or relating to establishing or maintaining business websites, such as S&S Auto Sales and Dennis Polk Equipment, advertising vehicles for sale, the offer or sale of vehicles including farming equipment, and photographs of vehicles of the type commonly used to advertise vehicles for sale;

b. Personal identifying information of individuals other than those residing at 4827 RIVERTON AVENUE, NORTH HOLLYWOOD, CALIFORNIA 91601, including social security numbers, other identifying numbers, dates of birth, addresses and telephone numbers, credit, gift, or debit card information, PINs, credit reports, and bank or other financial institution information, and records referring or relating to such information;

c. Counterfeit identity documents, such as passports and driver's licenses, whether blank, completed, or partially completed, and their components, such as seals, watermarks, security windows, official signatures or the cutting-and-pasting of signatures, holographic security features, ultraviolet printed features, raised micro dot features, and translucent Teslin printed design components, identification-proportioned photographs of faces, and programs or records referring or relating to them;

1 d. Credit and debit cards not in the names of the
2 residents of 4827 RIVERTON AVENUE, NORTH HOLLYWOOD, CA 91601, cards
3 with magnetic strips that are commonly overwritten to produce
4 counterfeit access devices, such as gift cards with no value on them
5 (which will be determined after the search) or blank card stock, any
6 card for which the embossing or information on the front does not
7 match the information recorded on the magnetic strip on the back
8 (which will be determined after the search), any card with a PIN
9 written on it or attached to it, lists of PINs, and records or
10 documents referring or relating to the same;

11 e. Equipment and objects used to skim, shim, or
12 counterfeit credit or debit cards, such as embossers, encoders,
13 ultraviolet printing devices, tipping foil, magnetic card readers or
14 writers, credit card chip readers and writers, blank cards containing
15 magnetic strips or chips, related equipment or materials such as
16 chips, magnetic strips, images of debit or credit cards, portable
17 media storage devices, holographic stickers, partially completed
18 credit or debit cards, and documents, records, or programs that refer
19 or relate to them;

20 f. Miniature or spy cameras or surveillance equipment
21 that could be used to capture PINs, equipment to install or mount
22 them, including magnets, or to record or transmit their images, and
23 documents, records, and programs, referring or relating to them
24 including the data they record;

25 g. Blank or partially completed credit and debit cards,
26 cards with magnetic strips that are commonly overwritten to produce
27 counterfeit access devices, such as gift cards with no value on them
28 (which will be determined after the search) or blank card stock, any

1 card for which the embossing or information on the front does not
2 match the information recorded on the magnetic strip on the back
3 (which will be determined after the search), any card with a PIN
4 written on it or attached to it, lists of PINs, and records or
5 documents referring or relating to the same;

6 h. Equipment designed to produce identity documents,
7 cards, or access devices, or their security features, such as card
8 printers, embossers, encoders, magnetic card readers or writers,
9 credit card chip readers and writers, their components and supplies,
10 such as blank card stock, tipping foil, Teslin sheets, holographic
11 printing supplies, ultraviolet printing supplies, and records or
12 programs that refer or relate to them;

13 i. Documents and records referring or relating to machine
14 shops, metal working, sheet metal, or the custom manufacture of
15 mechanical or electronic devices;

16 j. Records, programs, and items relating to the
17 counterfeiting or manipulation of documents and identifications, such
18 as the cutting-and-pasting of signatures, forging or copying
19 passports, driver's licenses, and other form of identification,
20 identification-proportioned photographs of faces, letterheads,
21 watermarks, and seals, including the altered or counterfeited
22 information itself.

23 k. Documents, records, and programs referring or relating
24 to ATMs including their locations and cash withdrawals or advances,
25 and pay/owe sheets;

26 l. Documents, records, and programs referring or
27 relating to international transfers of funds, international travel or
28 visas including illegal border crossing and the smuggling of persons,

1 international shipping or packages, foreign financial accounts, and
2 citizenship or alienage;

3 m. Documents, records, and images showing members of the
4 conspiracy associating or communicating with each other or with the
5 unidentified persons also captured on ATM surveillance photographs;

6 n. Documents and records referring or relating to the
7 conversion of cash to financial instruments such as checks and wire
8 transfers, and vice versa, for a percentage of the dollar value
9 converted, or the transfer of cash abroad, such as through Hawalas or
10 money transferring businesses, like Western Union, or the purchase of
11 cryptocurrency for cash;

12 o. Mail matter and shipping packages, opened or unopened,
13 not addressed to or from 4827 RIVERTON AVENUE, NORTH HOLLYWOOD, CA
14 91601, and documents or records referring or relating to the same;

15 p. Currency, prepaid debit or credit cards, and casino
16 chips with a value in excess of \$1,000, including the first \$1,000 if
17 more than \$1,000 is found;

18 q. Documents and keys relating to public storage units,
19 rental cars, prepaid cellular telephones, safety deposit boxes,
20 Commercial Mail Receiving Agencies, or receiving mail or deliveries
21 at someone else's address;

22 r. Records referring or relating to counter surveillance
23 of law enforcement, jail or prison, arrests, criminal investigations,
24 criminal charges, asset forfeiture, investigations by financial
25 institutions, and the threatened or actual closure of accounts by
26 financial institutions;

27 s. Documents and records referring or relating to
28 currency transaction reports (CTRs), their reporting thresholds,

1 attempting to structure cash transactions to avoid CTRs, cash
2 transactions totaling over \$10,000 even if conducted in lesser
3 increments, or the purchase of more than \$3,000 of postal money
4 orders in a two-week period, or conducting multiple cash ATM
5 transactions or purchasing multiple postal money orders on the same
6 day;

7 t. Documents and records referring or relating to the
8 conversion of cash to financial instruments such as checks and wire
9 transfers, and vice versa, for a percentage of the dollar value
10 converted, or the transfer of cash abroad, such as through Hawalas or
11 money transferring businesses, like Western Union, or the purchase of
12 cryptocurrency for cash;

13 u. Records relating to wealth and the movement of wealth
14 since 2022, such as tax returns and forms, crypto-currency accounts
15 and transfers, other digital wealth storage and transfer methods
16 including PayPal and Venmo, money orders, brokerage and financial
17 institution statements, wire transfers, currency exchanges, deposit
18 slips, cashier's checks, transactions involving prepaid cards, and/or
19 other financial documents related to depository bank accounts, lines
20 of credit, credit card accounts, real estate mortgage initial
21 purchase loans or loan refinances, residential property leases,
22 escrow accounts, the purchase, sale, or leasing of automobiles or
23 real estate, or auto loans, and investments, or showing or referring
24 to purchases or transactions for more than \$1,000;

25 v. Records or items containing indicia of occupancy,
26 residency or ownership of any location or vehicle being searched,
27 such as keys, rental agreements, leases, utility bills, identity
28 documents, cancelled mail, and surveillance video;

1 w. Documents and records showing electronic and telephone
2 contacts and numbers called or calling, such as SIM cards, address
3 books, call histories, telephone bills, and Signal, ICQ, Telegram,
4 and email addresses.

5 x. Cryptocurrency and related records and items, such as
6 those referring or relating to public or private keys or addresses,
7 or cryptocurrency wallets or their parts, including "recovery seeds"
8 or "root keys" which may be used to regenerate a wallet. Seizure of
9 the cryptocurrency and wallets will be accomplished by transferring
10 or copying them to a public cryptocurrency address controlled by the
11 United States, or by restoring them onto computers controlled by the
12 United States.

13 y. Any digital device which is itself or which contains
14 evidence, contraband, fruits, or instrumentalities of the SUBJECT
15 OFFENSES, and forensic copies thereof.

16 2. With respect to any digital device containing evidence
17 falling within the scope of the foregoing categories of items to be
18 seized:

19 a. evidence of who used, owned, or controlled the device
20 at the time the things described in this warrant were created,
21 edited, or deleted, such as logs, registry entries, configuration
22 files, saved usernames and passwords, documents, browsing history,
23 user profiles, e-mail, e-mail contacts, chat and instant messaging
24 logs, photographs, and correspondence;

25 b. evidence of the presence or absence of software that
26 would allow others to control the device, such as viruses, Trojan
27 horses, and other forms of malicious software, as well as evidence of
28

1 the presence or absence of security software designed to detect
2 malicious software;

3 c. evidence of the attachment of other devices;

4 d. evidence of counter-forensic programs (and associated
5 data) that are designed to eliminate data from the device;

6 e. evidence of the times the device was used;

7 f. passwords, encryption keys, biometric keys, and other
8 access devices that may be necessary to access the device;

9 g. applications, utility programs, compilers,
10 interpreters, or other software, as well as documentation and
11 manuals, that may be necessary to access the device or to conduct a
12 forensic examination of it;

13 h. records of or information about Internet Protocol
14 addresses used by the device;

15 i. records of or information about the device's Internet
16 activity, including firewall logs, caches, browser history and
17 cookies, "bookmarked" or "favorite" web pages, search terms that the
18 user entered into any Internet search engine, and records of user
19 typed web addresses.

20 3. As used herein, the terms "records," "documents,"
21 "programs," "applications," and "materials" include records,
22 documents, programs, applications, and materials created, modified,
23 or stored in any form, including in digital form on any digital
24 device and any forensic copies thereof.

25 4. As used herein, the term "digital device" includes any
26 electronic system or device capable of storing or processing data in
27 digital form, including central processing units; desktop, laptop,
28 notebook, and tablet computers; personal digital assistants; wireless

1 communication devices, such as telephone paging devices, beepers,
2 mobile telephones, and smart phones; digital cameras; gaming consoles
3 (including Sony PlayStations and Microsoft Xboxes); peripheral
4 input/output devices, such as keyboards, printers, scanners,
5 plotters, monitors, and drives intended for removable media; related
6 communications devices, such as modems, routers, cables, and
7 connections; storage media, such as hard disk drives, floppy disks,
8 memory cards, optical disks, and magnetic tapes used to store digital
9 data (excluding analog tapes such as VHS); and security devices.

10 **II. SEARCH PROCEDURE FOR DIGITAL DEVICES**

11 5. In searching digital devices or forensic copies thereof,
12 law enforcement personnel executing this search warrant will employ
13 the following procedure:

14 a. Law enforcement personnel or other individuals
15 assisting law enforcement personnel (the "search team") will, in
16 their discretion, either search the digital device(s) on-site or
17 seize and transport the device(s) and/or forensic image(s) thereof to
18 an appropriate law enforcement laboratory or similar facility to be
19 searched at that location. The search team shall complete the search
20 as soon as is practicable but not to exceed 120 days from the date of
21 execution of the warrant. The government will not search the digital
22 device(s) and/or forensic image(s) thereof beyond this 120-day period
23 without obtaining an extension of time order from the Court.

24 b. The search team will conduct the search only by using
25 search protocols specifically chosen to identify only the specific
26 items to be seized under this warrant.

27 i. The search team may subject all of the data
28 contained in each digital device capable of containing any of the

1 items to be seized to the search protocols to determine whether the
2 device and any data thereon falls within the list of items to be
3 seized. The search team may also search for and attempt to recover
4 deleted, "hidden," or encrypted data to determine, pursuant to the
5 search protocols, whether the data falls within the list of items to
6 be seized.

7 ii. The search team may use tools to exclude normal
8 operating system files and standard third-party software that do not
9 need to be searched.

10 iii. The search team may use forensic examination and
11 searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit),
12 which tools may use hashing and other sophisticated techniques.

13 c. If the search team, while searching a digital device,
14 encounters immediately apparent contraband or other evidence of a
15 crime outside the scope of the items to be seized, the team will not
16 search for similar evidence outside the scope of the items to be
17 seized without first obtaining authority to do so.

18 d. If the search determines that a digital device does
19 not contain any data falling within the list of items to be seized,
20 the government will, as soon as is practicable, return the device and
21 delete or destroy all forensic copies thereof.

22 e. If the search determines that a digital device does
23 contain data falling within the list of items to be seized, the
24 government may make and retain copies of such data, and may access
25 such data at any time.

26 f. If the search determines that a digital device is
27 (1) itself an item to be seized and/or (2) contains data falling
28 within the list of other items to be seized, the government may

1 retain the digital device and any forensic copies of the digital
2 device, but may not access data falling outside the scope of the
3 other items to be seized (after the time for searching the device has
4 expired) absent further court order.

5 g. The government may also retain a digital device if the
6 government, prior to the end of the search period, obtains an order
7 from the Court authorizing retention of the device (or while an
8 application for such an order is pending), including in circumstances
9 where the government has not been able to fully search a device
10 because the device or files contained therein is/are encrypted.

11 h. After the completion of the search of the digital
12 devices, the government shall not access digital data falling outside
13 the scope of the items to be seized absent further order of the
14 Court.

15 6. The review of the electronic data obtained pursuant to this
16 warrant may be conducted by any government personnel assisting in the
17 investigation, who may include, in addition to law enforcement
18 officers and agents, attorneys for the government, attorney support
19 staff, and technical experts. Pursuant to this warrant, the
20 investigating agency may deliver a complete copy of the seized or
21 copied electronic data to the custody and control of attorneys for
22 the government and their support staff for their independent review.

23 7. In order to search for data capable of being read or
24 interpreted by a digital device, law enforcement personnel are
25 authorized to seize the following items:

26 a. Any digital device capable of being used to commit,
27 further, or store evidence of the offense(s) listed above;

1 b. Any equipment used to facilitate the transmission,
2 creation, display, encoding, or storage of digital data;

3 c. Any magnetic, electronic, or optical storage device
4 capable of storing digital data;

5 d. Any documentation, operating logs, or reference
6 manuals regarding the operation of the digital device or software
7 used in the digital device;

8 e. Any applications, utility programs, compilers,
9 interpreters, or other software used to facilitate direct or indirect
10 communication with the digital device;

11 f. Any physical keys, encryption devices, dongles, or
12 similar physical items that are necessary to gain access to the
13 digital device or data stored on the digital device; and

14 g. Any passwords, password files, biometric keys, test
15 keys, encryption codes, or other information necessary to access the
16 digital device or data stored on the digital device

17 a. During the execution of this search warrant, law
18 enforcement is permitted to: (1) depress the thumbs and/or fingers of
19 MIHAI TRIF, and any other adult located at the SUBJECT PREMISES
20 during the execution of the search who is reasonably believed by law
21 enforcement to be a user of a biometric sensor-enabled device that
22 falls within the scope of the warrant, onto the fingerprint sensor of
23 the device (only when the device has such a sensor), and direct which
24 specific finger(s) and/or thumb(s) shall be depressed; and (2) hold
25 the device in front of the faces of those persons with their eyes
26 open to activate the facial-, iris-, or retina-recognition feature,
27 in order to gain access to the contents of any such device. In
28 depressing a person's thumb or finger onto a device and in holding a

1 device in front of a person's face, law enforcement may not use
2 excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989);
3 specifically, law enforcement may use no more than objectively
4 reasonable force in light of the facts and circumstances confronting
5 them.

6 8. The special procedures relating to digital devices found in
7 this warrant govern only the search of digital devices pursuant to
8 the authority conferred by this warrant, and do not apply to any
9 other search of digital devices.

1 **AFFIDAVIT**

2 I, Jenae Combest-Smith being duly sworn, declare and state as
3 follows:

4 **INTRODUCTION**

5 1. I am a Special Agent with Homeland Security Investigations
6 ("HSI") in Los Angeles, California, and have been so employed since
7 May 2022. To become an HSI Special Agent, I completed six months of
8 training at the Federal Law Enforcement Training Center in Brunswick,
9 Georgia.

10 2. During my employment as an HSI Special Agent, I have
11 participated in investigations related to narcotics smuggling,
12 organized criminal activity, document fraud, sex trafficking, human
13 smuggling, and other financial related crimes. I have participated in
14 various aspects of criminal investigations, including telephone
15 records analysis, physical surveillance, search warrants, seizures of
16 narcotics, electronics, documents, skimming devices, and reviewing
17 evidence from those seizures. I have also spoken to and interacted
18 with many law enforcement agents who have prior knowledge and
19 experience investigating financial related crimes and the methods
20 used to commit those crimes.

21 3. Prior to becoming a Special Agent with HSI, I was employed
22 as an insurance fraud investigator for approximately 12 years in the
23 private sector. During my employment as an insurance fraud
24 investigator, I investigated fraudulent insurance claims and was
25 responsible for reporting fraudulent claims to designated government
26 and law enforcement agencies for further investigation and
27 prosecution
28

1 4. I also have extensive experience investigating Romanian
2 Transnational Criminal Organizations (TCO). I have conducted
3 investigations in the Los Angeles area related to various fraud
4 crimes and money laundering, and I have also traveled to Romania to
5 share information and coordinate investigations with HSI Bucharest
6 and Romanian law enforcement regarding Romanians who travel from
7 Romania and Europe to the United States to defraud victims.

8 **I. PURPOSE OF AFFIDAVIT: SEARCH WARRANTS**

9 5. This affidavit is made in support of search warrants for
10 the residence and vehicle of MIHAI TRIF for evidence of conspiracy to
11 commit mail, wire, and bank fraud, money laundering, and passport
12 fraud, in violation of Title 18 U.S.C. §§ 1341, 1343, 1344, 1349,
13 1956, and 1546 (collectively, the "SUBJECT OFFENSES"), as described
14 in Attachment B.

15 6. The information set forth in this affidavit is based upon
16 my participation in the investigation, encompassing my personal
17 knowledge, observations and experience, as well as information
18 obtained through my review of evidence, investigative reports, and
19 information provided by others, including other law enforcement
20 partners. As this affidavit is being submitted for the limited
21 purpose of securing the requested warrants, I have not included each
22 and every fact known to me concerning this investigation. I have set
23 forth only the facts that I believe are necessary to establish
24 probable cause for the requested warrants.

25 **II. PREMISES AND VEHICLE TO BE SEARCHED**

26 7. The premises and vehicle to be searched are:
27
28

1 a) The residence located at 4827 RIVERTON AVENUE, NORTH
2 HOLLYWOOD, CALIFORNIA 91601 (the "**SUBJECT RESIDENCE**"), described
3 more fully in Attachment A-1, which is incorporated by
4 reference.

5 b) The BLACK 2024 LAND ROVER RANGE ROVER SPORT P400
6 BEARING California license plate 9MNG093, VIN SAL1L9FU5RA404809,
7 registered to EAN Holdings, and driven by MIHAI TRIF ("**SUBJECT**
8 **VEHICLE**"), described more fully in Attachment A-2, which is
9 incorporated by reference.

10 **III. ADDITIONAL INFORMATION ABOUT FINANCIAL FRAUD**

11 8. I have conducted financial investigations involving
12 sophisticated money laundering techniques and fraud. Through training
13 and experience, I have become familiar with how those engaged in
14 fraudulent activity obtain identifying information of victims, such
15 as a full name, date of birth and social security number, and then
16 use that information to open numerous bank and credit card accounts.
17 I know that individuals that commit fraud maintain victim information
18 and other information relevant to the fraud scheme for long periods
19 of time because it is of value in perpetuating additional acts or
20 further fraud schemes. The purpose of opening accounts (i.e., bank,
21 email, phone, etc.) is to further a fraud scheme, which often
22 involves several co-conspirators. The goal of this scheme is to
23 defraud banks, merchants, and victims to obtain cash or other items
24 of monetary value such as gift cards and electronics. These items are
25 often sought out due to their high liquidity. During account
26 openings, those individuals committing fraud typically provide
27 fictitious and/or fraudulent identities and a mailing address that
28

1 they exercise control over to obtain a bank issued debit or credit
2 card in furtherance of the fraud scheme, often using post mailboxes
3 or third-party mail receipt services to elude detection by law
4 enforcement. Due to the complexity of the fraud, the sheer number of
5 victims, and criminal conduct spanning multiple jurisdictions, it is
6 not uncommon for these financial fraud crimes go unsolved and/or
7 uninvestigated. This scheme requires the perpetrators to be in
8 communication, which is often done via cell phone(s) and/or VoIP
9 phones. Additionally, those involved in fraudulent acts and schemes
10 generally use a computer to facilitate the scheme by setting up email
11 accounts, setting up VoIP accounts, applying for bank accounts and
12 credit cards online, or other necessary things to make the scheme
13 successful, such as manufacturing counterfeit identification
14 documents, altered and/or counterfeit checks, credit cards, or other
15 financial instruments.

16 **IV. ADDITIONAL INFORMATION ABOUT ROMANIAN TRANSNATIONAL CRIMINAL**
17 **ORGANIZATIONS (TCO)**

18 9. Members of Romanian TCOs are trained to travel from Romania
19 and Europe to the United States to defraud Americans, United States
20 government programs, and the United States banking system. Members of
21 Romanian TCOs often stay in the United States illegally for many
22 years while they commit these crimes. Oftentimes, members travel back
23 and forth from the United States but re-enter and exit illegally in
24 order to evade law enforcement. Members are trained to import
25 fraudulent identification documents to assist them with their crimes
26 and launder money for the TCO with the goal to re-integrate it into
27 the Romanian banking system and real estate. This has been
28

1 corroborated by intelligence received from Romanian law enforcement
2 along with my training and experience on Romanian TCOs.

3 10. Members of Romanian TCO fraud groups typically enter the
4 country either legally with a visa, if they have no criminal record
5 and can pose as a legitimate tourist or businessperson, or through
6 established immigrant-smuggling rings in Mexico and Canada otherwise.
7 Oftentimes the crew members maintain false identity documents, which
8 they use if arrested to make it harder to identify them. Some
9 maintain false passports so that they can abscond if granted bail and
10 flee the country.

11 11. Members of Romanian TCO fraud groups have various ways of
12 handling the proceeds of their offenses. Some is kept in cash for
13 routine expenses. Some is usually deposited into a local bank
14 account to pay for items for which cash would raise suspicion, such
15 as rental cars and housing. The bulk, however, is sent abroad either
16 to their co-conspirators or home countries. This may be as simple as
17 sending cash hidden among other items abroad through carriers such as
18 DHL, or transfers through banks, Hawalas, Western Union, or similar
19 services. More recently, the trend has been to purchase
20 cryptocurrencies for cash.

21 12. Members of Romanian TCOs involved in fraud schemes must
22 keep evidence of their schemes, such as contact information for their
23 co-conspirators, lists of victim information and accounts used in the
24 scheme, simply to keep the scheme going. Much of this evidence is
25 now stored on digital devices such as computers and smartphones.

26 13. Generally, perpetrators of fraud and identity theft schemes
27 maintain this evidence where is close at hand and safe, such as in
28

1 their residences, automobiles, and, especially with smartphones, on
2 their person. For larger or more sophisticated frauds, participants
3 often attempt to distance themselves from some of the incriminating
4 evidence by renting public storage units or safety deposit boxes
5 where they often keep the items they will not need immediate access
6 to.

7 14. Members of Romanian TCOs must out of necessity communicate
8 with one another. Commonly this is done by text, VOIP, email,
9 telephone, or specialty communication application, often an encrypted
10 one such as WhatsApp, and most often by smartphone. Members of the
11 conspiracy commonly carry their smartphones, which include the
12 contact information for their co-conspirators, on or near their
13 persons, such as in their cars or residences.

14 **V. STATEMENT OF PROBABLE CAUSE**

15 15. Homeland Security Investigations (HSI) Los Angeles, HSI
16 Pensacola, HSI Attaché Bucharest, HSI Attaché Vienna, United States
17 Secret Service (USSS) San Diego, and Romanian Law Enforcement
18 (hereinafter collectively referred to as "Investigators") are
19 currently investigating a Romanian Transnational Criminal
20 Organization (TCO). I am the assigned case agent and have been
21 directly involved with the investigation for approximately 18 months.

22 16. In summary, the investigation has revealed that members of
23 this Romanian TCO operate various organized crimes groups that have
24 specializations including human smuggling, narcotics smuggling, money
25 laundering, import and export violations, organized retail theft,
26 gambling, prostitution, violence, credit-card skimming, and financial
27 fraud schemes domestically and internationally. Investigators have
28

1 identified numerous members of this Romanian TCO, including a
2 Romanian national identified as MIHAI TRIF, DOB: XX/XX/1993.

3 17. The investigation to date has revealed that TRIF likely
4 unlawfully entered the United States within the last 24 months, most
5 likely from Canada. Specifically, I have received information from
6 Canadian authorities showing that TRIF entered Canada via Montreal
7 International Airport on September 9, 2022, from Paris, France. TRIF
8 was granted entry into Canada as a visitor and used a valid Romanian
9 passport.

10 18. I have conducted queries in law enforcement databases and
11 have been unable to locate any lawful entry and subsequent admission
12 into the United States after TRIF's entry into Canada on September 9,
13 2022. Based on my training and experience, I know that it is common
14 practice for members of Romanian TCOs and other illegal aliens
15 engaged in criminal activity to enter the United States illegally
16 through Canada or Mexico in order to evade law enforcement. Thus, TRIF
17 is illegally present in the United States with no lawful status.

18 19. In the United States, TRIF has at least two arrests with no
19 dispositions in California, including a February 2023 misdemeanor
20 arrest for Petty Theft and a June 2023 felony arrest for Inflict
21 Corporal Injury to Spouse / Cohabitant, referencing FBI No XXXXXXPAL
22 and California State ID XXXXX888. The prosecution status of both
23 cases is currently unknown to me. As detailed herein, these arrests
24 were made after TRIF unlawfully entered the United States at some
25 time after September 9, 2022. Despite TRIF's immigration status, the
26 arresting agencies had no legal authority to question TRIF's
27 immigration status. Additionally, TRIF was arrested in the state of
28

1 California, which is regarded as a "sanctuary state".¹ Thus,
2 immigration authorities were not aware of TRIF's arrest and
3 subsequent temporary detention.

4 20. As detailed herein, Investigators and my subsequent
5 investigation have identified at least 15 fraudulent and fictitious
6 identities directly attributable to TRIF and TRIF's fraud schemes.
7 Several of the identities were identified prior to TRIF using them
8 (i.e., actively targeting inbound international shipments that seized
9 the fraudulent documents), several of the identities were identified
10 after-the-fact as part of a historical financial investigation, and
11 at least two are currently being proactively investigated as newly
12 assumed identities that TRIF is believed to be actively using,
13 including one as part of a new Confidence Fraud Scheme (i.e., "Karel
14 TOKAR") and another as an identity TRIF is using to launder illicit
15 proceeds and elude detection by law enforcement (i.e., "Ivan
16 BUGATZI").

17 21. For purposes of this affidavit, I have conducted an in-
18 depth analysis of TRIF's three most recent identities, including
19 "Marek BALVIN", "Karel TOKAR", and "Ivan BUGATZI". These three
20 identities are recent and relevant to my ongoing investigation into
21 TRIF and TRIF's fraud schemes several ways and encompasses the
22 relevant period of August - Present.

23 22. At this time, TRIF's full role in the fraud schemes is
24 currently unknown; however, the investigation revealed that TRIF at a
25 minimum is responsible for creating fictitious and fraudulent

26
27 ¹ In April 2017, the California State Senate approved a bill
28 that increased protections for immigrants. The measure prohibits
local law enforcement agencies from using resources to investigate,
detain, report or arrest people for immigration violations.

1 identities and opening and maintaining financial accounts used to
2 directly receive wire transfers from victims. TRIF then immediately
3 withdraws and spends the funds from swindled victims. While it
4 appears that TRIF is organizing the scheme, based on my training,
5 experience, and investigation to date, I believe that TRIF's fraud
6 schemes are complex and likely involves multiple unknown co-
7 conspirators. For example, some victims reported talking to both a
8 male and female scammer by telephone.

9 23. First, "Marek BALVIN" was identified as an identity used to
10 swindle at least six victims out of \$141,278 in September 2024 using
11 two U.S. financial institutions, including Wells Fargo Account
12 XXXXXX5272 ("WF 'BALVIN' Account-5272") and Citibank Account
13 XXXXX7684 ("Citibank 'BALVIN' Account-7684"). Both accounts were
14 opened in August 2024 in the greater Los Angeles, CA area using the
15 fictitious identity and supporting fraudulent documents of "Marek
16 BALVIN". I have provided still frame CCTV images from the Citibank
17 'BALVIN' Account-7684 showing that an individual I have identified by
18 sight as TRIF was captured opening the account on August 22, 2024,
19 and subsequently withdrawing funds via teller and ATM from the
20 account on September 9, 11, 13, and 17, 2024. The fund source was
21 from two separate victims that wired \$15,000 and \$16,000 on or about
22 September 9, 2024. The two victims were confirmed through victim
23 interviews and identified in North Dakota and New Jersey,
24 respectively. The victim funds were immediately withdrawn by TRIF
25 from a branch and ATM located less than 4 miles from the **SUBJECT**
26 **RESIDENCE**.

24. Second, "Karel TOKAR" was identified as a new replacement identity used by TRIF as part of a new and ongoing fraud scheme. I identified "Karel TOKAR" by conducting an analysis of the identity "Marek BALVIN," including a phone analysis and other investigative techniques. The subsequent analysis identified the identity of "Karel TOKAR" and the suspected cellular phone attributable to the identity, identified as (818) 605-2154 ("TRIF's 'TOKAR' Phone-2154"). I positively identified TRIF as the user and holder of TRIF's 'TOKAR' Phone-2154 via subsequent court authorization geolocation of TRIF's 'TOKAR' Phone-2154 in conjunction with physical surveillance in November 2024 and other investigative techniques. This also assisted in identifying the **SUBJECT RESIDENCE** and the **SUBJECT VEHICLE**. The identification of "Karel TOKAR" was exclusively established by the initial identification of "Marek BALVIN". This is strong evidence to indicate that the identities are intertwined and directly related to each other.

25. Third, "Ivan BUGATZI" was identified as TRIF's alias to launder his illicit proceeds and to live day-to-day in an attempt to elude detection by law enforcement. I identified "Ivan BUGATZI" by court authorization geolocation of TRIF's 'TOKAR' Phone-2154 in conjunction with physical surveillance and a review of CCTV footage in November 2024. These investigative techniques allowed Investigators to identify the identity of "Ivan BUGATZI", the **SUBJECT RESIDENCE**, the **SUBJECT VEHICLE**, and the suspected cellular phone attributable to the identity, identified as (310) 482-0611 ("TRIF's 'BUGATZI' Phone-0611"). I positively identified TRIF as the user and holder of TRIF's 'BUGATZI' Phone-0611 via subsequent court

1 authorization geolocation of TRIF's 'BUGATZI' Phone-0611 in
2 conjunction with physical surveillance in November 2024 and other
3 investigative techniques. The identification of "Ivan BUGATZI" was
4 exclusively established by the initial identification of "Marek
5 BALVIN" and the subsequent identification of "Karel TOKAR". This is
6 strong evidence to indicate that the identities are intertwined and
7 directly related to each other.

8 26. TRIF's fictitious identities were also supported by
9 fraudulently created and/or altered foreign passports and other
10 identity documents, which were frequently often used to open U.S.
11 bank accounts and other records, including at Wells Fargo, Citibank,
12 Bank of America, and JP Morgan Chase Bank. Most, if not all, of the
13 bank accounts identified during the investigation were opened in
14 and/or had money withdrawn from the account(s) in the Central
15 District of California. Investigators have confirmed that the
16 passports are fraudulent and the identities are fictitious; however,
17 some of the passport numbers were legitimately issued at some point
18 and subsequently altered. Investigators also discovered that TRIF
19 often digitally enhanced and/or modified his self-image on the
20 fraudulent identity documents. Thus, often the individual photograph
21 on the passport (or other document(s)) appeared slightly different
22 but was determined to be TRIF based on several investigative
23 techniques, computer software, and international cooperation with
24 Romanian authorities. For example, the altered photo would change the
25 hair style, hair length, facial hair (i.e., mustache, beard, goatee),
26 and the general facial characteristics (i.e., face shape, eye
27 placement, etc.) Based on my training and experience, I know that

1 computer, specialized computer software, and some level of expertise
2 is required to alter photographs. I believe TRIF did this in an
3 attempt to elude detection by law enforcement and to obfuscate the
4 investigation and the subsequent ability of law enforcement to
5 identify TRIF.

6 27. For example, Investigators and my subsequent investigation
7 detailed herein have identified at least 15 identities created and/or
8 used by TRIF and likely other co-conspirators as part of TRIF's
9 overall fraud schemes. Investigators have confirmed TRIF as the
10 creator of these fictitious and fraudulent identities several ways,
11 including coordination with Romanian law enforcement, the use of
12 facial recognition and other software, seizures attributable to
13 addresses utilized by TRIF (and other aliases), and the investigation
14 to date. I have also reviewed numerous images used on the below
15 documents and have determined that the individual depicted is TRIF. I
16 am familiar with the physical attributes and appearance of TRIF by
17 sight. The identities directly attributable to TRIF were as follows:

- 18 • Antonin LOUIS, COB: France, DOB: XX/XX/1992, PP Number XXXXX5060
19 (France); and,
- 20 • Sofiane MAX, COB: France, DOB: XX/XX/1992, PP Number XXXXX2440
21 (France); and,
- 22 • Claude GAUTHIER, COB: France, DOB: XX/XX/1990, PP Number
23 XXXXX6367 (France); and,
- 24 • Haden GOOSSENS, COB: Belgium, DOB: XX/XX/1990, PP Number
25 XXXX0878 (Belgium); and,
- 26 • Noah ARTHUR, COB: Belgium, DOB: XX/XX/1995, PP Number XXXX5421
27 (Belgium) ; and,

- 1 • Danuser BUCHER, COB: Switzerland, DOB: XX/XX/1990, PP Number
- 2 XXXX9109 (Switzerland); and,
- 3 • Leon RUSU, COB: Canada, DOB: XX/XX/1990, PP Number XXXX8022
- 4 (Canada); and,
- 5 • Tiberiu ENZO - DOB: Netherlands, DOB: Unknown, PP Number
- 6 XXXXK193; and,
- 7 • Axel MULLER - DOB: Germany, DOB: Unknown, PP Number XXXXXR86
- 8 • Glenn GREENFIELD - Unknown, NFI ("No Further Information")
- 9 • Aurelio ROTH - Unknown, NFI
- 10 • David HUGO, COB: Luxemburg, DOB: XX/XX/1991, PP Number XXXXV7K4
- 11 (Luxemburg); and,
- 12 • Marek BALVIN, COB: Czech Republic, DOB: XX/XX/1994, PP Number
- 13 XXXX7084 (Czech Republic); and,
- 14 • Karel TOKAR, COB: Czech Republic, DOB: XX/XX/1989, PP Number
- 15 XXXX5348 (Czech Republic); and,
- 16 • Ivan BUGATZI, COB: Canada, DOB: XX/XX/1991, PP Number XXXX9334,
- 17 Canadian driver's license XXXXXXXXX9109.

18 28. Investigators have conducted physical surveillance, served
 19 administrative summons, conducted interviews, spoken with other law
 20 enforcement officers, executed court authorized searches and
 21 seizures, conducted international controlled deliveries, reviewed
 22 financial records, and various other investigative techniques as part
 23 of the ongoing investigation into TRIF and TRIF's Confidence Fraud
 24 Schemes and TRIF's fictitious and fraudulent identities.

25 29. My subsequent investigation has identified at least five
 26 separate financial fraud schemes committed and/or being committed by
 27 MIHAI TRIF and likely other known and unknown co-conspirators using
 28

1 fictitious and fraudulently created identities between approximately
2 March 2023 - Present, including "Marek BALVIN," and "Karel TOKAR". My
3 investigation has also identified TRIF's "clean" fictitious and
4 fraudulent identity that TRIF likely uses for day-to-day living.
5 Based on my training, experience, and investigation to date, I
6 believe that TRIF has compartmentalized his identities used in fraud
7 schemes (i.e., "Marek BALVIN", "Karel TOKAR", and others) from his
8 "clean" day-to-day identity (i.e., "Ivan BUGATZI") to elude detection
9 by law enforcement. For purposes of the affidavit, I have conducted
10 an in-depth analysis of "Marek BALVIN", "Karel TOKAR", and "Ivan
11 BUGATZI", as detailed below.

12 **VI. SUMMARY OF FRAUD SCHEMES COMMITTED BY TRIF AND OTHERS**

13 30. Based on my training and experience, the fraud schemes
14 committed by TRIF and other unknown co-conspirators can be referred
15 to as a Confidence Fraud Scheme. In general, a Confidence Fraud
16 Scheme is a sophisticated plot to deceive and/or defraud individuals
17 into giving money or other personal information to a scammer.
18 Scammers often use a variety of methods to gain the trust of their
19 victims, including building relationships, creating a sense of trust,
20 and exploiting vulnerabilities.

21 31. In this case, TRIF and likely other unknown co-conspirators
22 purported to be a seller(s) of a piece of heavy-duty equipment (i.e.,
23 a Kubota L39 backhoe loader tractor) or a vintage restored vehicle
24 (i.e., a 1965 Chevrolet C-10) on a spoofed website² and/or on

25
26 ² Website spoofing is a scam where cyber criminals create a
27 website that closely resembles a trusted brand as well as a domain
28 that is virtually identical to a brand's web domain. The goal of
website spoofing is to lure a brand's customers, suppliers, partners
and employees to a fraudulent website and convince them to share
sensitive information like login credentials, Social Security

1 Facebook Marketplace³. Ultimately, there was no tractor or vehicle
2 for sale and sole purpose of the scheme was to swindle victims of
3 their money. TRIF's Confidence Fraud Scheme was then layered with
4 other information used to deceive potential victims into believing
5 the purported sale of the item was authentic, including the use of a
6 spoofed and/or legitimate appearing websites (i.e., "Dennis Polk
7 Equipment" and "S&S Auto Sales"), the use of several VoIP phone
8 numbers⁴ to communicate with the victims in various capacities (i.e.,
9 the dealerships, the shipper, etc.), the use of a shipping and other
10 companies to coordinate the sale and/or the "transport" of the
11 vehicle to the victim (i.e., BENSON C EQUIPMENT LLC, DP EQUIPMENT
12 LLC, OUTLET RETAIL ONE, LLC, and STALLION CARGO AZ LLC), a use of The
13 UPS Store Post Mailboxes (PMBs) (i.e., The UPS Store #5391 in
14 Commerce, CA in the name of "Sofiane MAX", The UPS Store #0015 in
15 Huntington Beach, CA and The UPS Store #0012 in Los Angeles, CA in
16 the name of "Antonin LOUIS", The UPS Store #5626 in Sun Valley, CA in
17 the name of "Marek BALVIN", and The UPS Store #3272 in Stevenson
18 Ranch, CA in the name of "Karel TOKAR", and The UPS Store #4466 in
19 Long Beach, CA in the name of "Ivan BUGATZI"), and at least four U.S.

20
21 numbers, credit card information or bank account numbers.
22 Additionally, a spoofed website can also be used to give the
23 appearance of the purported business and/or business activity to
24 appear legitimate.

25 ³ Facebook Marketplace is classified-ad section of the social
26 network that specializes in helping individuals and businesses sell
27 items locally. Marketplace is Facebook's expansion into markets to
28 compete with services like eBay, Craigslist, and other similar
platforms.

29 ⁴ Voice over Internet Protocol (VoIP) is a technology that
allows users to make phone calls and other communications over the
internet instead of a traditional phone line. VoIP can be used on a
variety of devices, including computers, smartphones, and VoIP
phones.

1 financial institutions in furtherance of the fraud scheme (i.e., Bank
2 of America, JP Morgan Chase Bank, Wells Fargo, and Citibank).⁵

3 32. The investigation revealed that TRIF would generally use
4 these fraudulent and fictitious identities and related accounts for
5 30-90 days as part of a fraud scheme and then transition to a newly
6 established fictitious identity once the fraud scheme was fruitful
7 and financially benefited TRIF, i.e., a victim(s) was swindled out of
8 money and TRIF successfully received / withdrew the funds. This
9 constant transition and creation of new identities has made it
10 difficult for law enforcement to proactively identify and investigate
11 TRIF and TRIF's fraud schemes in real time. Thus, Investigators are
12 often investigating TRIF's crimes historically, i.e., after they have
13 already occurred and TRIF has transitioned to a new identity.
14 Additionally, the high-quality fraudulent identity documents created
15 and used by TRIF and TRIF's apparent knowledge base regarding the use
16 of technology to defraud victims has also made it more difficult for
17 law enforcement to investigate. This is evidenced by TRIF's ability
18 to continuously and successfully open bank accounts at U.S. financial
19 institutions and elude detection by law enforcement for more than 18
20 months.

21 **VII. VICTIM IDENTIFICATION AND INFORMATION RELATED TO TRIF AND**
22 **OTHERS' CONFIDENCE FRAUD SCHEMES**

23 33. My and other Investigators continued investigation into
24 TRIF and TRIF's related Confidence Fraud Schemes have identified a
25 total of 14 victims with a total loss of \$351,806 in ten different
26 states, including Alabama, California, Illinois, Kansas, Kentucky,

27 ⁵ Bank of America, JP Morgan Chase Bank, Wells Fargo, and
28 Citibank are federally insured by the Federal Deposit Insurance
Corporation (FDIC) and therefore meets the federal definition of a
"financial institution" pursuant to 18 U.S.C. §20.

1 Missouri, Nevada, New Jersey, North Dakota, and Oklahoma. The victims
2 were defrauded between approximately May 2023 - September 2024.

3 34. As part of the investigation, Investigators and/or I have
4 confirmed that the victims were in fact victims of TRIF's Confidence
5 Fraud Schemes several ways. Specifically, Investigators and/or I have
6 spoken with local law enforcement, interviewed more than 10 of the
7 victims, interviewed at least one family member of a victim, have
8 reviewed at least eight of the filed police reports detailing the
9 incidents, have reviewed supporting bank records detailing the wire
10 transfers, and conducted additional investigative follow up. Based on
11 my training, experience, and investigation to date, I believe all
12 identified 14 victims were victims of a Confidence Fraud Scheme
13 perpetrated by TRIF and likely other unknown co-conspirators. I am
14 intentionally being vague about the names and other unique
15 identifying of the victims to protect the identities of the victims.

16 35. Generally, banks are obligated to refund money lost to
17 fraud (i.e., identity theft, credit card fraud, etc.); however, banks
18 may deny the refund if the customer was negligent or involved in the
19 scam. Thus, in this case, all victims were at a *complete financial*
20 *loss because the wire transfers were originated by the victim.*
21 Additionally, at least two victims are currently making monthly
22 payments on loans that were obtained to fund the wire transfers in
23 TRIF's Confidence Fraud Scheme.

24 36. I have learned through the continued investigation that the
25 losses sustained by each individual victim was substantial, including
26 emotionally and financially. In general, a lot of the victims used
27 their life savings and/or took out a loan to purchase an item that
28

1 would benefit themselves, their current business, and/or a new
2 business. Often, the victims were in small towns (i.e., less than
3 5,000 people) and were directly and/or indirectly involved in
4 construction, agriculture, or other employment.

5 37. For example, one of the victims was identified as a Captain
6 at a local police department in the greater California area. Despite
7 this victim's extensive police training and experience, he/she was
8 successfully swindled out of approximately \$20,000. I also identified
9 at least two victims that had not even reported the crime because of
10 shame and embarrassment. Based on my training and experience, I
11 believe this is strong evidence to support my belief of TRIF's
12 Confidence Fraud Schemes were sophisticated.

13 38. Specifically, between approximately March - May 2023 TRIF
14 used the identity "Sofiane MAX" and related fictitious business BENSON
15 C EQUIPMENT LLC to open and maintain business bank accounts Bank of
16 America Account-9289 ("BoFA 'MAX' Account-9289") and JP Morgan Chase
17 Account-8985 ("JPMC 'MAX' Account-8985"). These two accounts were
18 used to receive funds from at least five victims out of \$146,131. The
19 funds were immediately withdrawn, spent, and/or transferred in the
20 greater Los Angeles, CA area.

21 39. Between approximately March - May 2023 TRIF used the
22 identity "Antonin LOUIS" and related fictitious business DP EQUIPMENT
23 LLC to open and maintain business bank account Citibank Account-0721
24 ("Citibank 'LOUIS' Account-0721"). This account was used to receive
25 funds from at least two victims out of \$43,747. The funds were
26 immediately withdrawn, spent, and/or transferred in the greater Los
27 Angeles, CA area.

1 40. Between approximately November - December 2023 TRIF used
2 the identity "Leon RUSU" and related fictitious business OUTLET
3 RETAIL ONE, LLC to open and maintain business bank account Bank of
4 America Account-6936 ("BoFA 'RUSU' Account-6936"). This account was
5 used to receive funds from at least one victim out of \$20,650. The
6 funds were immediately withdrawn, spent, and/or transferred in the
7 greater Los Angeles, CA area.

8 ***Identification and Analysis of "Marek BALVIN"***

9 41. As detailed herein, the investigation identified the
10 fictitious and fraudulent identity of "Marek BALVIN" as being TRIF. The
11 identification of "Marek BALVIN" started from a reported fraud scam
12 that occurred in the greater Bismarck, North Dakota area using a
13 Citibank account. HSI Bismarck subsequently initiated the
14 investigation into fraud scam. The fraud scam was the same modus
15 operandi as TRIF's Confidence Fraud Scams. HSI Bismarck's subsequent
16 investigation and case coordination then overlapped with my
17 investigation into TRIF and other known and unknown co-conspirators.
18 HSI Vienna also assisted in the investigation because of the Czech
19 Republic passport that identified. The investigation then expanded
20 and identified a second bank account in the name of "Marek BALVIN" at
21 Wells Fargo.

22 42. In summary, I learned that between approximately June -
23 September 2024, TRIF used the identity "Marek BALVIN" and related
24 fictitious business STALLION CARGO AZ LLC to open and maintain business
25 bank accounts WF 'BALVIN' Account-5272 and Citibank 'BALVIN' Account-
26 7684. These accounts were used to receive funds from at least six
27 victims out of \$141,278, including two victims initially identified
28

1 by an HSI Bismarck investigation. Both accounts were opened in August
2 2023 in the greater Los Angeles, CA area using the fictitious identity
3 and supporting fraudulent documents of "Marek BALVIN".

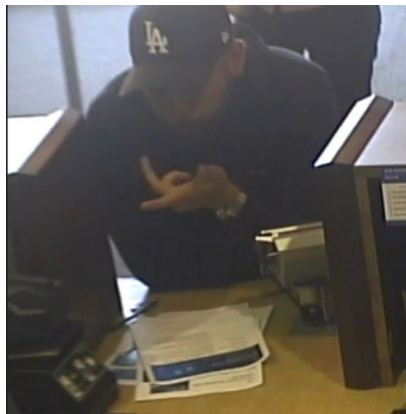
4 43. As shown below, I have provided still frame CCTV images
5 from the Citibank 'BALVIN' Account-7684 showing that an individual I
6 have identified by sight as TRIF was captured opening the account on
7 August 22, 2024, and subsequently withdrawing funds via teller and
8 ATM from the account on September 9, 11, 13, and 17, 2024. The fund
9 source was from two separate victims that wired \$15,000 and \$16,000
10 on or about September 9, 2024. The two victims were identified as
11 residing in North Dakota and New Jersey and were confirmed as victims
12 through victim interviews by HSI Bismarck. A subsequent review of
13 bank records for Citibank 'BALVIN' Account-7684 showed that the
14 victim funds were immediately withdrawn by TRIF from a branch and
15 ATM. The bank branch for all the transactions occurred at the
16 Citibank located at 360 E Magnolia Burbank, CA 91502 ("Citibank
17 Burbank"), which is less than 4 miles from the **SUBJECT RESIDENCE**.
18 Additionally, a review of the ATM CCTV footage from September 17,
19 2024, showed TRIF arrived and departed on an e-scooter. As detailed
20 herein, this identical scooter was later observed in the trunk of the
21 **SUBJECT VEHICLE** on November 13, 2024, at a car wash in Arcadia, CA.
22 The positive identification of TRIF as the sole individual that
23 opened, maintained, and withdrew funds from the account is strong
24 evidence to indicate TRIF's direct involvement in the Confidence
25 Fraud Schemes.

26 44. An image of an individual I identified by sight as TRIF
27 opening Citibank 'BALVIN' Account-7684 on August 22, 2024, is
28

1 depicted below. The account was opened at Citibank Burbank, which was
2 less than 4 miles to the **SUBJECT RESIDENCE**. The image looked like
3 this:



4
5
6
7
8
9 45. An image of an individual I identified by sight as TRIF
10 withdrawing funds from Citibank 'BALVIN' Account-7684 on September
11 11, 2024, is depicted below. The funds that were withdrawn were funds
12 from an identified victim of a Confidence Fraud Scheme. The funds
13 were withdrawn from Citibank Burbank less than 4 miles to the **SUBJECT**
14 **RESIDENCE**. It also appeared that during the transaction TRIF
15 presented what appeared to be a passport for identification
16 verification purposes. Based on my training and experience, I believe
17 TRIF presented the fictitious and fraudulent passport in the name of
18 "Marek BALVIN". The image looked like this:



46. Several images of an individual I identified by sight as TRIF withdrawing funds from Citibank 'BALVIN' Account-7684 ATM in September 2024, is depicted below. The funds were withdrawn from Citibank Burbank, which was less than 4 miles to the **SUBJECT RESIDENCE**. The funds that were withdrawn were funds from an identified victim of a Confidence Fraud Scheme. In summary, TRIF arrived, withdrew funds using a card from TRIF's wallet, and subsequently departed on an e-scooter. The images looked like this:



47. As detailed herein, the identification and subsequent investigation into the fictitious and fraudulent identity of "Marek BALVIN" was the catalyst that assisted law enforcement in identifying the fictitious and fraudulent identifies "Karel TOKAR" and "Ivan BUGATZI". As detailed below, the investigation confirmed that TRIF was the sole individual directly attributable to "Karel TOKAR" and "Ivan BUGATZI".

48. As part of the ongoing investigation, on November 7, 2024, United States Magistrate Judge Maria A. Audero authorized a Search and Seizure Search Warrant for prospective live tracking via GPS coordinates and historical information associated with TRIF's 'TOKAR' Phone-2154. The warrant authorized prospective live tracking via GPS

1 coordinates for 45 days and historical information for 30 days from
2 the date of warrant, referencing case number 2:24-MJ-6739. The phone
3 number was directly attributable to the fictitious and fraudulent
4 identity of "Karel TOKAR".

5 49. Between approximately November - 13, 2024, I did not
6 receive any geolocation information for TRIF's 'TOKAR' Phone-2154.
7 Based on my training and experience, this was consistent with the
8 phone being powered off. Then, on November 13, 2024, between
9 approximately 9:59 a.m. PST to 5:29 p.m. PST, the phone powered on
10 and geolocation was received in 10-minute increments. The following
11 day, on November 14, 2024, HSI Vienna SA C. Lindsly conducted a
12 review and analysis of the geolocation information received. As
13 detailed below, SA Lindsly's subsequent analysis of the limited data
14 received pursuant to the court authorized geolocation identified
15 several locations the phone was located at, including Fasching's Car
16 Wash, 425 N Santa Anita Ave, Arcadia, CA 91006 (Fasching's Car Wash)
17 and a parking lot at Arcadia Mall. The geolocation information
18 received was very accurate, including +/- 8 meters. This subsequently
19 allowed law enforcement to collect and review CCTV footage from both
20 locations which assisted the investigation several ways. First, a
21 review of the CCTV footage confirmed that TRIF was the holder of
22 TRIF's 'TOKAR' Phone-2154. Second, it identified TRIF's vehicle as
23 the **SUBJECT VEHICLE**. Third, it identified another previously unknown
24 alias, identified herein as "Ivan BUGATZI".

25 50. An image of an individual I identified by sight as TRIF and
26 the **SUBJECT VEHICLE** on November 13, 2024, at Fasching's Car Wash is
27 depicted below. Of note, I identified an e-scooter in the trunk of
28

1 the SUBJECT VEHICLE consistent with the e-scooter TRIF used to
2 withdraw funds from Citibank 'BALVIN' Account-7684 in September,
3 2024. The image of TRIF and the **SUBJECT VEHICLE** (with the e-scooter
4 in the trunk) looked like this:



5
6
7
8
9
10
11 51. Subsequent record checks revealed that TRIF's Range Rover
12 was an Enterprise rental car rented on October 3, 2024, to "Ivan
13 BUGATZI" and that "Ivan BUGATZI" (i.e., TRIF) is paying approximately
14 \$4,000 per month to rent TRIF's Range Rover. To date, TRIF still has
15 an active rental agreement with Enterprise with an expected return
16 date of November 28, 2024, according to their business records. The
17 **SUBJECT VEHICLE** was rented using the fictitious and fraudulent
18 identify of "Ivan BUGAZTI" and paid for using a related Bank of
19 America account, as detailed herein. The Bank of America account and
20 related information is detailed below. I have also reviewed a CCTV
21 still frame on October 3, 2024, from Enterprise and confirmed that
22 the purported renter "Ivan BUGATZI" was in fact TRIF. An image of an
23 individual I identified by sight as TRIF and the **SUBJECT VEHICLE**
24 departing Enterprise on October 3, 2024, is depicted below. The image
25 looked like this:
26
27
28



52. The continued investigation into "Ivan BUGATZI" identified Bank of America Account number XXXXXXXXXXXX3857 ("BofA 'BUGATZI' Account-3857") and Bank of America credit card number XXXXXXXXXXXX0602 ("BofA 'BUGATZI' CC-0602") as accounts currently being used by "Ivan BUGATZI" (i.e., TRIF). Investigators have reviewed and discussed with an authorized representative the two Bank of America accounts attributable to "Ivan BUGAZTI".

53. In summary, I learned that the accounts were opened on September 17, 2024, using the fictitious and fraudulent identity and supporting documents of "Ivan BUGATZI". In general, it appears that the two accounts are being used to live lavishly with likely illicit proceeds of swindled victims using other aliases and Confidence Fraud Schemes in the greater Los Angeles, CA area, i.e., rent high-end vehicles, travel, purchase expensive jewelry, dine at restaurants, etc. The two accounts generally maintained a low account balance and would have enough funds in the account to cover general day-to-day transactions, other purchases, and to make frequent payments on BofA 'BUGATZI' CC-0602. All the funds into the accounts were cash deposits either via ATM and/or teller deposits in the greater Los Angeles, CA area. The source of the funds is unknown; however, based on my

1 training and experience I believe that the funds are likely proceeds
2 of TRIF's Confidence Fraud Schemes.

3 54. Investigators also learned some of the purchases were as
4 follows: UberEATS, parking, Zelle payments, purchases at various
5 grocery stores, etc. There were also numerous payments to DDHD
6 Jewelry in Los Angeles, CA, including \$1,000 and \$2,000 payments on
7 November 18 and 19, respectively. Open-source queries revealed that
8 DDHD Jewelry was a high-end custom jewelry store with the motto, "You
9 Imagine It, We Bring it to Life". DDHD Jewelry also sold other
10 jewelry, including men's rings, bracelets, women's rings, chains,
11 earrings, pendants, etc. Based on my training, experience, and
12 investigation to date, I believe these payments were likely for
13 jewelry TRIF has ordered using proceeds from his known and unknown
14 Confidence Fraud Schemes, as detailed herein.

15 55. Investigators also learned that TRIF's Bank of America CC-
16 0602 also had regular day-to-day transactions, which were
17 subsequently paid off via BofA 'BUGATZI' Account-3857. The authorized
18 Bank of America representative stated that the activity of both
19 accounts generally would not raise any suspicion by banking
20 authorities. Based on my training and experience, I believe this low-
21 risk transactional activity was conducted by TRIF purposely to elude
22 detection by law enforcement and enable TRIF to use the identity of
23 "Ivan BUGATZI" for day-to-day living using illicit proceeds procured
24 from TRIF's Confidence Fraud Schemes.

25 **VIII. IDENTIFICATION OF THE SUBJECT RESIDENCE AND SUBJECT VEHICLE**

26 56. As detailed herein, I am investigating TRIF for the SUBJECT
27 OFFENSES. My investigation has spanned approximately 20 months and
28

1 has identified a sophisticated and complex fraud scheme perpetuated
2 by TRIF and other known and unknown co-conspirators. Over the span of
3 several months, Investigators and I have used numerous investigative
4 techniques in an attempt to disrupt TRIF's ongoing fraud schemes. A
5 primary objective of my ongoing investigation was to identify TRIF's
6 primary residence, potential stash locations, and vehicles used by
7 TRIF. As detailed below, the continued investigation has identified
8 the **SUBJECT RESIDENCE** and the **SUBJECT VEHICLE** as TRIF's primary
9 residence and vehicle, respectively.

10 57. Specifically, I have worked a historical and proactive
11 investigation to disrupt and dismantle TRIF's Confidence Fraud
12 Schemes and likely other fraud related activities. As detailed
13 herein, I have identified TRIF's "clean" identity as "Ivan BUGATZI".
14 The purpose of TRIF using "Ivan BUGATZI" is to launder illicit
15 proceeds and to elude detection by law enforcement.

16 58. As detailed above, my investigation identified several Bank
17 of America accounts attributable to "Ivan BUGATZI". A review of those
18 accounts identified numerous transactions billed by UberEATS,
19 including as recently as November 2024. Based on my training,
20 experience, and opensource queries, I know that UberEATS is an online
21 food ordering and delivery platform launched by the company Uber in
22 2014. The meals are delivered by couriers using various methods,
23 including cars, scooters, bikes, or on foot. UberEATS is operational
24 in over 6,000 cities in 45 countries as of 2021. Generally, a
25 customer of UberEATS use an application to order food. The use of the
26 UberEATS application requires a customer to create an account,
27 including customer name, address, cellular phone number, payment
28

1 method(s), and other information. The provided cellular phone number
2 is used in the event an UberEATS delivery person or the Uber driver
3 needs to contact the intended customer. Additionally, once an
4 UberEATS order is placed and subsequently delivered, UberEATS
5 maintains that delivery information, including restaurant, delivery
6 date and time, and delivery address, among other things.

7 59. Based in part on the aforementioned facts, on November 22,
8 2024, United States Magistrate Judge Alicia Rosenberg authorized a
9 2703(d) Court Order requesting records associated to cellular phone
10 number TRIF's 'BUGAZTI' Phone-0611 and customer name "Ivan BUGATZI".
11 The order authorized the requested records from the date of the
12 account(s) inception to date of order, referencing case number 2:24-
13 MJ-7053.

14 60. The following day, on or about November 23, 2024,
15 Investigators served the Court Order via Uber Technologies, Inc's
16 ("Uber") law enforcement portal, referencing internal Uber case
17 number 00498516.

18 61. The following day, on November 24, 2024, Investigators
19 received the records from UberEATS pursuant to the 2703(d) Court
20 Order. The records were received via Uber's law enforcement portal.

21 62. On the same day HSI Vienna SA Lindsly conducted an analysis
22 of the UberEATS records. I have spoken with SA Lindsly and conducted
23 an independent review of the records. The records received two files,
24 including a file titled "Response to Request - 00498516.pdf" and
25 "Attachment to Response - 00498516.xlsx".

26 63. In summary the records revealed that "Ivan BUGAZTI" (i.e.,
27 TRIF) had two separate UberEATS accounts, including Display Names
28

"Ivan Bugatzi" and "Ivan Bug". In summary, based on a review of the records it appears that TRIF used Display Name "Ivan Bugatzi" from approximately September 29 - October 15, 2024, and Display Name "Ivan Bug" from approximately October 16 - Present, 2024. This was corroborated by a review of IP address logs, customer information, and customer order information.

64. As detailed below, a review of the records identified TRIF's primary residence as the **SUBJECT RESIDENCE**. In summary, between September 29 - November 20, 2024, TRIF (using Display Names "Ivan Bugatzi" and "Ivan Bug") had a total of 17 food deliveries. 16 of the 17 food deliveries were delivered to the **SUBJECT RESIDENCE**. The only food delivery to an alternate address occurred on September 29, 2024, and was delivered to 310 Tahiti Way #201, Marina Del Rey, CA. Additionally, I reviewed the GPS coordinates submitted by the UberEATS delivery driver, which documented the exact location the food was delivered. The delivery GPS coordinates are consistent with the **SUBJECT RESIDENCE**. The order deliveries were as follows:

Account	Amount	Order Date / Time	Delivery Date / Time	Delivery Address
Ivan Bugatzi	\$74.36	2024-09-29 12:51:49	2024-09-29 13:33:48	310 Tahiti Way
Ivan Bugatzi	\$13.99	2024-10-01 9:21:22	2024-10-01 10:03:48	SUBJECT RESIDENCE
Ivan Bugatzi	\$41.91	2024-10-02 21:28:45	2024-10-02 22:26:00	SUBJECT RESIDENCE
Ivan Bug	\$23.92	2024-10-26 17:34:48	2024-10-26 17:48:46	SUBJECT RESIDENCE
Ivan Bug	\$39.46	2024-10-27 9:53:42	2024-10-27 10:27:46	SUBJECT RESIDENCE
Ivan Bug	\$121.45	2024-10-28 20:27:35	2024-10-28 21:21:28	SUBJECT RESIDENCE
Ivan Bug	\$32.96	2024-11-01 12:05:18	2024-11-01 12:53:20	SUBJECT RESIDENCE
Ivan Bug	\$17.98	2024-11-01 19:15:15	2024-11-01 20:00:08	SUBJECT RESIDENCE
Ivan Bug	\$81.97	2024-11-02 18:49:36	2024-11-02 19:37:52	SUBJECT RESIDENCE
Ivan Bug	\$18.96	2024-11-03 13:34:33	2024-11-03 14:10:35	SUBJECT RESIDENCE
Ivan Bug	\$61.80	2024-11-04 20:00:15	2024-11-04 20:52:35	SUBJECT RESIDENCE
Ivan Bug	\$81.97	2024-11-05 19:10:08	2024-11-05 19:53:08	SUBJECT RESIDENCE
Ivan Bug	\$25.15	2024-11-07 23:35:45	2024-11-07 23:48:54	SUBJECT RESIDENCE

Ivan Bug	\$86.83	2024-11-15 19:28:58	2024-11-15 20:26:00	SUBJECT RESIDENCE
Ivan Bug	\$24.94	2024-11-16 16:05:31	2024-11-16 17:07:42	SUBJECT RESIDENCE
Ivan Bug	\$40.99	2024-11-19 20:09:24	2024-11-19 21:08:28	SUBJECT RESIDENCE
Ivan Bug	\$21.96	2024-11-20 23:24:55	2024-11-20 23:44:15	SUBJECT RESIDENCE

65. As detailed herein, Investigators and I had identified TRIF's primary vehicle as the **SUBJECT VEHICLE** and TRIF's primary residence as the **SUBJECT RESIDENCE**. On November 25, 2024, at approximately 10:45 a.m. PST, HSI SA Yoo was conducting covert physical surveillance immediately in front of the **SUBJECT RESIDENCE**. In summary, SA Yoo observed the **SUBJECT VEHICLE** pull out of a dedicated gate that gave access to the **SUBJECT RESIDENCE**. Based on SA Yoo's training and experience, it appeared that the gate was only accessible by occupants of the small complex, including the **SUBJECT RESIDENCE**, likely by an electronic remote. I also conducted a review of court authorized geolocation information obtained from TRIF's 'TOKAR' Phone-2154 and TRIF's "BUGATZI" Phone-0611. A subsequent review of the geolocation information for both phones was consistent with TRIF arriving and departing the area of the **SUBJECT RESIDENCE** consistent with SA Yoo's physical observations. Thus, this corroborates the identification of the **SUBJECT RESIDENCE** and **SUBJECT VEHICLE** as TRIF's primary residence and primary vehicle.

TRIF Used Skimmed Debit Cards at ATMs

66. Per video footage provided to me by Beverly Hills Police Department, TRIF utilized a Bank of America ATM in Beverly Hills, CA on February 20, 2023. Bank of America advised me that TRIF had attempted to use three stolen EDD cards and one EBT card at the same Bank of America ATM on February 20, 2023. I personally reviewed video footage of TRIF at the Bank of America ATM and confirmed his identity as the individual who attempted to use the three stolen EDD cards and

one EBT card. (To identify TRIF from surveillance images, I compared them to Romanian passport photos of MIHAI TRIF which I received from Romanian law enforcement.) Based on my training and experience, I know that criminals utilize various skimming devices and tools to steal information from EBT and EDD account holders. Criminals involved in skimming crimes often place skimming devices on ATMs and credit-card machines in order to steal the account numbers of EBT and EDD cards. Criminals then utilize other devices to create duplicate debit-cards which contain the stolen EBT and EDD victims account numbers on them. Criminals then go to ATMs and attempt to drain those victims' EBT and EDD accounts, also known as "cash-outs," as TRIF was captured on video doing. Accordingly, persons involved in skimming, like TRIF, commonly have evidence of skimming in their vehicles and residences, such as skimmers, blank cards which can be re-encoded with victims' account information, access card reader-writers, spy cameras, and related equipment.

IX. TRIF IS PREPARING TO CHANGE RESIDENCES

67. While investigating the **SUBJECT RESIDENCE** online on November 26, 2024, I saw that it was advertised as being for rent. I called the listed number and pretended to be interested in renting it. In summary, I learned that the current tenant (i.e., TRIF) would be vacating it on November 29, 2024. Additionally, as detailed herein, a subsequent review of the Enterprise rental agreement showed that the **SUBJECT VEHICLE** is scheduled to be returned on November 28, 2024. Based on my training and experience, I believe it is likely that TRIF might be in the process of transitioning to a new identity. Thus, the requested warrant is time sensitive. On November 27, 2024,

1 I was watching the **SUBJECT RESIDENCE** and personally observed TRIF
2 exit the residence and then enter it again in the morning.

3 X. **TRAINING AND EXPERIENCE ON DIGITAL DEVICES⁶**

4 68. Based on my training, experience, and information from
5 those involved in the forensic examination of digital devices, I know
6 that the following electronic evidence, inter alia, is often
7 retrievable from digital devices:

8 a. Forensic methods may uncover electronic files or remnants
9 of such files months or even years after the files have been
10 downloaded, deleted, or viewed via the Internet. Normally, when a
11 person deletes a file on a computer, the data contained in the file
12 does not disappear; rather, the data remain on the hard drive until
13 overwritten by new data, which may only occur after a long period of
14 time. Similarly, files viewed on the Internet are often
15 automatically downloaded into a temporary directory or cache that are
16 only overwritten as they are replaced with more recently downloaded
17 or viewed content and may also be recoverable months or years later.

18 b. Digital devices often contain electronic evidence related
19 to a crime, the device's user, or the existence of evidence in other
20 locations, such as, how the device has been used, what it has been
21 used for, who has used it, and who has been responsible for creating
22 or maintaining records, documents, programs, applications, and

23
24 ⁶ As used herein, the term "digital device" includes any
25 electronic system or device capable of storing or processing data in
26 digital form, including central processing units; desktop, laptop,
27 notebook, and tablet computers; personal digital assistants; wireless
28 communication devices, such as paging devices, mobile telephones, and
smart phones; digital cameras; gaming consoles; peripheral
input/output devices, such as keyboards, printers, scanners,
monitors, and drives; related communications devices, such as modems,
routers, cables, and connections; storage media; and security
devices.

1 materials on the device. That evidence is often stored in logs and
2 other artifacts that are not kept in places where the user stores
3 files, and in places where the user may be unaware of them. For
4 example, recoverable data can include evidence of deleted or edited
5 files; recently used tasks and processes; online nicknames and
6 passwords in the form of configuration data stored by browser, e-
7 mail, and chat programs; attachment of other devices; times the
8 device was in use; and file creation dates and sequence.

9 c. The absence of data on a digital device may be evidence of
10 how the device was used, what it was used for, and who used it. For
11 example, showing the absence of certain software on a device may be
12 necessary to rebut a claim that the device was being controlled
13 remotely by such software.

14 d. Digital device users can also attempt to conceal data by
15 using encryption, steganography, or by using misleading filenames and
16 extensions. Digital devices may also contain "booby traps" that
17 destroy or alter data if certain procedures are not scrupulously
18 followed. Law enforcement continuously develops and acquires new
19 methods of decryption, even for devices or data that cannot currently
20 be decrypted.

21 69. Based on my training, experience, and information from
22 those involved in the forensic examination of digital devices, I know
23 that it is not always possible to search devices for data during a
24 search of the premises for a number of reasons, including the
25 following:

26 a. Digital data are particularly vulnerable to inadvertent or
27 intentional modification or destruction. Thus, often a controlled
28

1 environment with specially trained personnel may be necessary to
2 maintain the integrity of and to conduct a complete and accurate
3 analysis of data on digital devices, which may take substantial time,
4 particularly as to the categories of electronic evidence referenced
5 above. Also, there are now so many types of digital devices and
6 programs that it is difficult to bring to a search site all of the
7 specialized manuals, equipment, and personnel that may be required.

8 a) Digital devices capable of storing multiple gigabytes are
9 now commonplace. As an example of the amount of data this equates
10 to, one gigabyte can store close to 19,000 average file size (300kb)
11 Word documents, or 614 photos with an average size of 1.5MB.

12 70. The search warrant requests authorization to use the
13 biometric unlock features of a device, based on the following, which
14 I know from my training, experience, and review of publicly available
15 materials:

16 a. Users may enable a biometric unlock function on some
17 digital devices. To use this function, a user generally displays a
18 physical feature, such as a fingerprint, face, or eye, and the device
19 will automatically unlock if that physical feature matches one the
20 user has stored on the device. To unlock a device enabled with a
21 fingerprint unlock function, a user places one or more of the user's
22 fingers on a device's fingerprint scanner for approximately one
23 second. To unlock a device enabled with a facial, retina, or iris
24 recognition function, the user holds the device in front of the
25 user's face with the user's eyes open for approximately one second.

26 b) In some circumstances, a biometric unlock function will not
27 unlock a device even if enabled, such as when a device has been
28

1 restarted or inactive, has not been unlocked for a certain period of
2 time (often 48 hours or less), or after a certain number of
3 unsuccessful unlock attempts. Thus, the opportunity to use a
4 biometric unlock function even on an enabled device may exist for
5 only a short time. I do not know the passcodes of the devices likely
6 to be found in the search.

7 c) In my training and experience, the person who is in
8 possession of a device or has the device among his or her belongings
9 at the time the device is found is likely a user of the device.
10 However, in my training and experience, that person may not be the
11 only user of the device whose physical characteristics are among
12 those that will unlock the device via biometric features, and it is
13 also possible that the person in whose possession the device is found
14 is not actually a user of that device at all. Furthermore, in my
15 training and experience, I know that in some cases it may not be
16 possible to know with certainty who is the user of a given device,
17 such as if the device is found in a common area of a premises without
18 any identifying information on the exterior of the device. Thus, if
19 while executing the warrant, law enforcement personnel encounter a
20 digital device within the scope of the warrant that may be unlocked
21 using one of the aforementioned biometric features, the warrant I am
22 applying for would permit law enforcement personnel to, with respect
23 to every person who is located at the TARGET PREMISES during the
24 execution of the search who is reasonably believed by law enforcement
25 to be a user of a biometric sensor-enabled device that falls within
26 the scope of the warrant: (1) depress the person's thumb- and/or
27 fingers on the device(s); and (2) hold the device(s) in front of the

1 face of the person with his or her eyes open to activate the facial-,
2 iris-, and/or retina-recognition feature.

3 d) In my training and experience, Romanian TCO members often
4 reside together to better coordinate their efforts. This is
5 especially true for persons involved in fraud crimes as these crimes
6 often require specialized tools and equipment to create fraudulent
7 identification documents and the like.

8 71. Other than what has been described herein, to my knowledge,
9 the United States has not attempted to obtain this data by other
10 means.

11 XI. CONCLUSION

12 72. Based upon the foregoing facts and my training and
13 experience, I believe there is probable cause to believe that
14 evidence of conspiracy to commit mail, wire, and bank fraud, money
15 laundering, and passport fraud listed in Attachment B will be found
16 at the **SUBJECT RESIDENCE** and the **SUBJECT VEHICLE**.

17 Attested to by the applicant in
18 accordance with the requirements
19 of Fed. R. Crim. P. 4.1 by
20 telephone on this ____ day of
21 November, 2024.

22 _____
23 UNITED STATES MAGISTRATE JUDGE
24
25
26
27
28